



Oslo kommune

Informasjonssikkerhet og digitalisering

Noen erfaringer fra Oslo kommune

26.04.2019

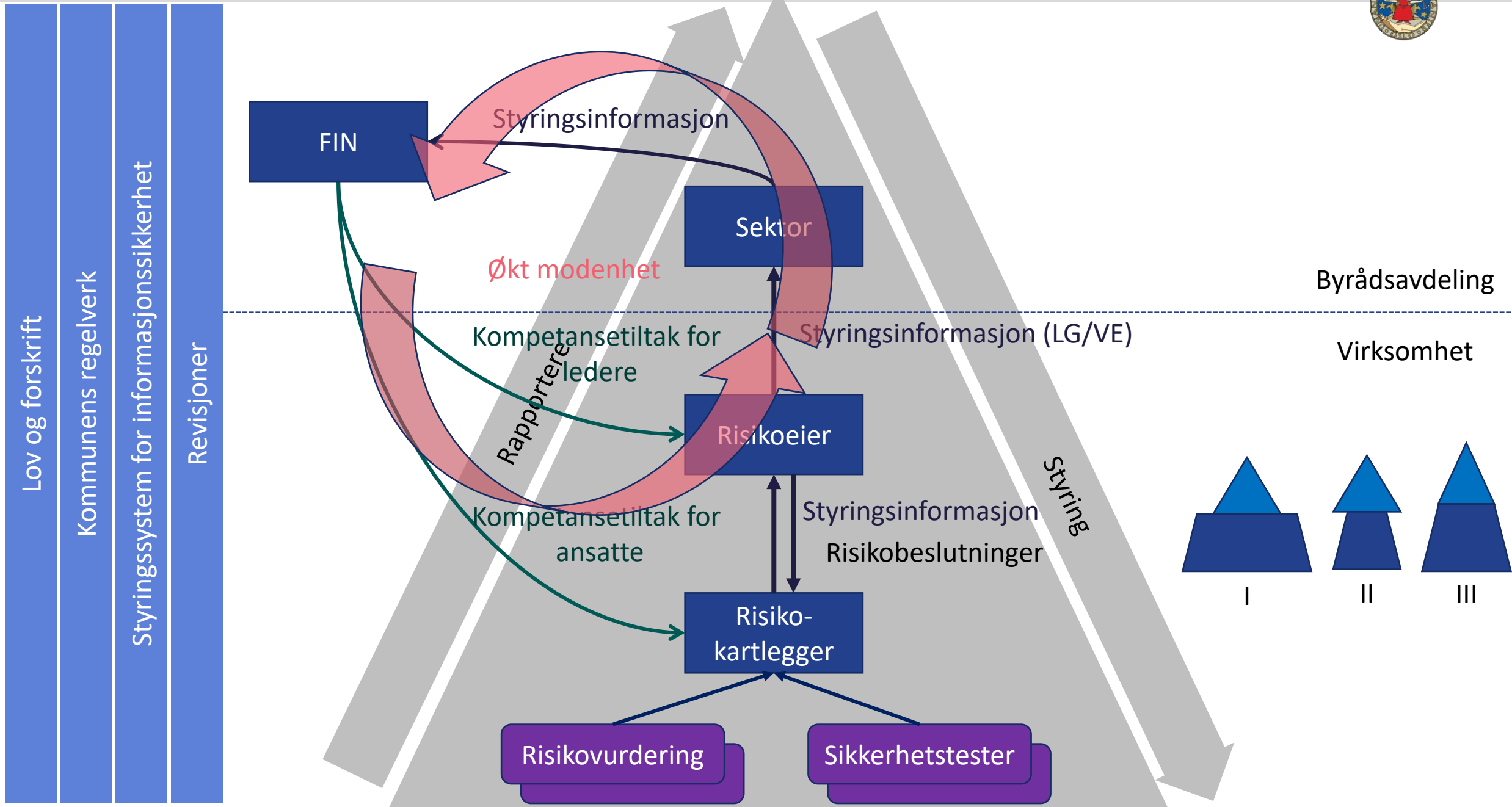
Lise Arneberg og Rune Schumann
Byrådsavdeling for finans, Oslo kommune



Oslo kommune

God risikostyring forutsetter kompetanse
og
kompetanse bygger vi gjennom erfaring

Risikotilnærming til informasjonssikkerhet og kompetanse





Oslo kommune

Informasjonssikkerhet og risiko i utviklingen digitale tjenester



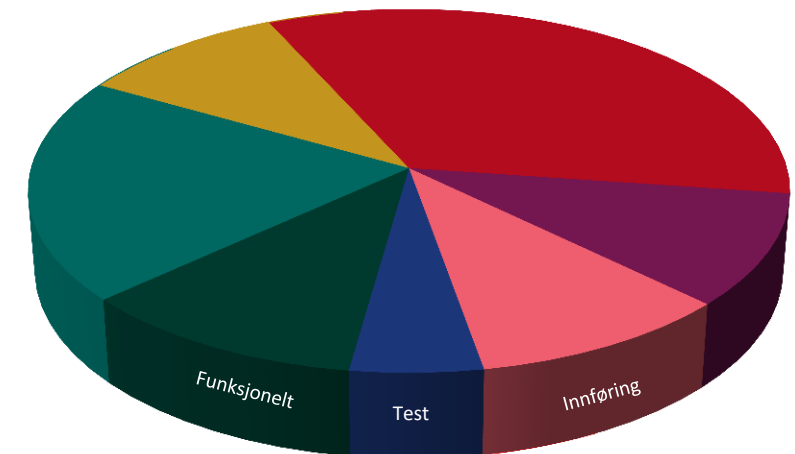
Behov for informasjonssikkerhetskompetanse i prosjektene

Informasjonssikkerhetsoppgaver:

1	Finnes det en oppdatert behandlingsoversikt som dekker tjenesten?
2	Er det gjort en vurdering av behovet for å vurdere konsekvenser for de registrertes personvern (fra nå referert til som DPIA)?
3	Hvis det er identifisert behov for DPIA, er denne utført og dokumentert?
4	Foreligger det en ROS-analyse som viser hvilken risiko som er identifisert i den ferdige Tjenesten?
5	Er det fastsatt krav til hva som skal anses som akseptabel risiko for Tjenesten?
6	Er systemeiers virksomhetsleder informert om eventuell uakseptabel (rød) risiko i Tjenesten og hvilke planer som finnes for å redusere slik risiko?
7	Er det gjennomført en sikkerhetstest/inntrengningstest av Tjenesten? Vennligst begrunn hvorfor hvis slik test ikke er gjennomført.
8	Er prinsippene for innebygget personvern ivaretatt ved utforming av Tjenesten?

9	Er det etablert en forvaltningsorganisasjon for Tjenesten? Er det avklart hvem som har ansvar for jevnlig kartlegging og vurdering av risiko gjennom sikkerhetstesting og ROS-analyser? Er det avsatt midler til disse tiltakene i forvaltningen?
10	Hvis Tjenesten har en ekstern leverandør av programvare, er det inngått avtale om sikkerhetsvedlikehold av denne programvaren?
11	Hvis Tjenesten ikke har et avtalefestet sikkerhetsvedlikehold, er ansvaret for å identifisere nødvendig sikkerhetsvedlikehold plassert og finansiert? (Slikt løpende vedlikehold er nødvendig også som følge av at det jevnlig oppdages sårbarheter i protokoller eller programvarebiblioteker som Tjenesten benytter.)
12	Er det etablert en forvaltningsorganisasjon for Tjenesten som har ansvar for løpende utførelse av sikkerhetsoppdatering av programvare og driftsmiljø.
13	Hvis Tjenesten, eller deler av denne, er levert av en ekstern leverandør eller driftes utenfor Oslo kommune, er det inngått Databehandlertavtaler?

Prosjektbemanning:



Tilsvarende er det også behov for informasjonssikkerhetskompetanse i drift og forvaltning



Oslo kommune

Leverandører
«Skal *informasjonssikkerhet* bestemme hvilken
leverandør vi skal velge?»

Publikumsløsninger og risiko

- Risikovurdering må gjøres i starten av anskaffelsesprosessen
- Før systemet kan tas i bruk må det gjennomføres sikkerhetstest
- Bruke leverandører som har kompetanse på sikkerhet





Oslo kommune

Informasjonssikkerhet som en del av virksomhetsstyringen



Risikostyring er kjent fra andre områder

Sykefravær øker brått og kraftig

Risiko:

- risiko for at virksomheten ikke oppnår sine målsetninger, at man ikke kan levere tjenester i henhold til lover og regler.
- risiko for presseoppslag om uheldige arbeidsforhold.

Akseptabel risiko:

- fastsatte mål om maksimalt sykefravær

Analyse:

- kartlegginger og undersøkelser for å finne årsaken.

Tiltak:

- sette inn tiltak for å få sykefraværet ned.

Antall sikkerhetsbrudd øker

Risiko:

- risiko for at virksomheten ikke oppnår sine målsetninger, at man ikke kan levere tjenester i henhold til lover og regler.
- risiko for presseoppslag om brudd på personvern

Akseptabel risiko:

- fastsatte mål om maksimalt antall sikkerhetsbrudd

Analyse:

- kartlegginger og undersøkelser for å finne årsaken.

Tiltak:

- sette inn tiltak for å få antall sikkerhetsbrudd ned.



Oslo kommune

Takk for oppmerksomheten!